



機能のライセンスと仕様

この付録では、機能のライセンスと仕様について説明します。この付録は、次の項で構成されています。

- 「サポートされているプラットフォームと機能」(P.A-1)
- 「セキュリティ サービス モジュール サポート」(P.A-10)
- 「VPN 仕様」(P.A-10)

サポートされているプラットフォームと機能

このソフトウェア バージョンでは、次のプラットフォームをサポートしています。各モデルの機能サポートについては、関連の表を参照してください。

- ASA 5505、表 A-1
- ASA 5510、表 A-2
- ASA 5520、表 A-3
- ASA 5540、表 A-4
- ASA 5550、表 A-5
- PIX 515/515E、表 A-6
- PIX 525、表 A-7
- PIX 535、表 A-8



(注)

イタリック体で示された項目は、基本ライセンスを変更できる個別のオプションライセンスです。ライセンスは組み合わせることができます。たとえば、10 セキュリティ コンテキスト ライセンスと Strong Encryption ライセンス、500 WebVPN ライセンスと GTP/GPRS ライセンス、または 4 つのライセンスをすべて同時に使用することができます。

表 A-1 ASA 5505 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5505	基本ライセンス		セキュリティ プラス	
ユーザ、同時 ¹	10	オプションのライセンス： 50 無制限	10	オプションのライセンス： 50 無制限
セキュリティ コンテキスト	サポートなし		サポートなし	
VPN セッション ²	10 の組み合わせた IPSec と WebVPN		25 の組み合わせた IPSec と WebVPN	
最大 IPSec セッション数	10		25	
最大 WebVPN セッション数	2	オプション ライセンス : 10	2	オプション ライセンス : 10
VPN ロード バランシング	サポートなし		サポートなし	
フェールオーバー	なし		アクティブ/スタンバイ (ステートフルフェールオーバーなし)	
GTP/GPRS	サポートなし		サポートなし	
最大 VLAN/ゾーン	3 (2 つの正規ゾーンともう 1 つの制限ゾーンだけが他の 1 つのゾーンと通信可能)		20	
最大 VLAN トランク数	サポートなし		無制限	
ファイアウォールの同時接続 ³	10 K		25 K	
最大物理インターフェイス数	無制限、VLAN/ゾーンに割り当て済み		無制限、VLAN/ゾーンに割り当て済み	
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)
RAM の最小値	128 MB		128 MB	

- ルーテッドモードの場合、内部（ビジネス VLAN およびホーム VLAN）のホストは、それらが外部（インターネット VLAN）と通信する場合（内部が外部への接続を開始した場合、および外部が内部への接続を開始した場合を含む）に、制限に対してカウントされます。外部が内部への接続を開始した場合でも、外部ホストは制限に対してカウントされず、内部ホストだけがカウントされることに注意してください。ビジネスとホーム間のトラフィックを開始するホストも制限に対してカウントされません。デフォルト ルートに関連付けられたインターフェイスは、外部インターネット インターフェイスと見なされます。デフォルト ルートがない場合、すべてのインターフェイス上のホストが制限値にカウントされます。トランスペアレント モードでは、ホスト数が最小のインターフェイスがホスト制限値にカウントされず、ホストの制限を表示するには、**show local-host** コマンドを参照してください。
- IPSec セッションと WebVPN セッションの最大数の合計が、VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
- 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80 % TCP と 20 % UDP のトラフィック混合に基づいています。

表 A-2 ASA 5510 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5510	基本ライセンス					セキュリティ プラス						
ユーザ、同時	無制限					無制限						
セキュリティ コンテキスト	サポートなし					2	オプションのライセンス :					
							5					
VPN セッション ¹	250 の組み合わせた IPSec と WebVPN					250 の組み合わせた IPSec と WebVPN						
最大 IPSec セッション数	250					250						
最大 WebVPN セッション数	2	オプションのライセンス :				2	オプションのライセンス :					
		10	25	50	100	250		10	25	50	100	250
VPN ロード バランシング	サポートなし					サポートなし						
フェールオーバー	なし					アクティブ/スタンバイまたはアクティブ/アクティブ						
GTP/GPRS	サポートなし					サポートなし						
最大 VLAN 数	50					100						
ファイアウォールの同時接続 ²	50 K					130 K						
最大物理インターフェイス数	(7.2(1) の場合) 10/100 に 3 つと管理トラフィック専用の管理インターフェイス (7.2(2) 以降の場合) 無制限					無制限 (7.2(3) 以降の場合) Ethernet 0/0 および Ethernet 0/1 は、ギガビットイーサネットインターフェイスとして使用されます。						
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)				基本 (DES)	オプション ライセンス : 強化 (3DES/AES)					
最小 RAM 容量	256 MB					256 MB						

1. IPSec セッションと WebVPN セッションの最大数の合計が、VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-3 ASA 5520 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5520	基本ライセンス							
ユーザ、同時	無制限				無制限			
セキュリティ コンテキスト	2	オプションのライセンス :						
		5	10	20				
VPN セッション ¹	750 の組み合わせた IPSec と WebVPN							
最大 IPSec セッション数	750							
最大 WebVPN セッション数	2	オプションのライセンス :						
		10	25	50	100	250	500	750
VPN ロード バランシング	サポートあり							
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ							
GTP/GPRS	なし	オプション ライセンス : イネーブル						
最大 VLAN 数	150							
ファイアウォールの同時接続 ²	280 K							
最大物理インターフェイス数	無制限							
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)						
最小 RAM 容量	512 MB							

1. IPSec セッションと WebVPN セッションの最大数の合計が、VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-4 ASA 5540 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5540	基本ライセンス										
ユーザ、同時	無制限					無制限					
セキュリティ コンテキスト	2	オプション ライセンス :									
		5	10	20	50						
VPN セッション ¹	5000 の組み合わせた IPSec と WebVPN										
最大 IPSec セッション数	5000										
最大 WebVPN セッション数	2	オプションのライセンス :									
		10	25	50	100	250	500	750	1000	2500	
VPN ロード バランシング	サポートあり										
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ										
GTP/GPRS	なし	オプション ライセンス : イネーブル									
最大 VLAN 数	200										
ファイアウォールの同時接続 ²	400 K										
最大物理インターフェイス数	無制限										
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)									
最小 RAM 容量	1 GB										

1. IPSec セッションと WebVPN セッションの最大数の合計が、VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-5 ASA 5550 適応型セキュリティ アプライアンス ライセンスの機能

ASA 5550	基本ライセンス										
ユーザ、同時	無制限										
セキュリティ コンテキスト	2	オプション ライセンス :									
		5	10	20	50						
VPN セッション ¹	5000 の組み合わせた IPSec と WebVPN										
最大 IPSec セッション数	5000										
最大 WebVPN セッション数	2	オプションのライセンス :									
		10	25	50	100	250	500	750	1000	2500	5000
VPN ロード バランシング	サポートあり										
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ										
GTP/GPRS	なし	オプション ライセンス : イネーブル									
最大 VLAN 数	250										
ファイアウォールの同時接続 ²	650 K										
最大物理インターフェイス数	無制限										
暗号化	基本 (DES)	オプション ライセンス : 強化 (3DES/AES)									
最小 RAM 容量	4 GB										

1. IPSec セッションと WebVPN セッションの最大数の合計が、VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切にすることができます。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

表 A-6 PIX 515/515E セキュリティ アプライアンス ライセンスの機能

PIX 515/515E	R (制限付き)		UR (制限なし)		FO (フェールオーバー) ¹		FO-AA (フェールオーバーアクティブ/アクティブ) ¹	
ユーザ、同時	無制限		無制限		無制限		無制限	
セキュリティ コンテキスト	サポートなし		2	オプション ライセンス : 5	2	オプション ライセンス : 5	2	オプション ライセンス : 5
IPSec セッション	2000		2000		2000		2000	
WebVPN セッション	サポートなし		サポートなし		サポートなし		サポートなし	
VPN ロード バランシング	サポートなし		サポートなし		サポートなし		サポートなし	
フェールオーバー	サポートなし		アクティブ/スタンバイ アクティブ/アクティブ		アクティブ/スタンバイ		アクティブ/スタンバイ アクティブ/アクティブ	
GTP/GPRS	なし	オプション ライセンス : イネーブル	なし	オプション ライセンス : イネーブル	なし	オプション ライセンス : イネーブル	なし	オプション ライセンス : イネーブル
最大 VLAN 数	10		25		25		25	
ファイアウォールの同時接続 ²	48 K		130 K		130 K		130 K	
最大物理インターフェイス数	3		6		6		6	
暗号化	なし	オプション ライセンス :	なし	オプション ライセンス :	なし	オプション ライセンス :	なし	オプション ライセンス :
		基本 (DES)		強化 (3DES/AES)		基本 (DES)		強化 (3DES/AES)
最小 RAM 容量	64 MB		128 MB		128 MB		128 MB	

- このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアだけで使用できます。どちらの装置も同じモデルである必要があります。
- 同時ファイアウォール接続は、4つの接続すべてに対して1つのホストと1つのダイナミック変換を持つ80% TCPと20% UDPのトラフィック混合に基づいています。

表 A-7 PIX 525 セキュリティ アプライアンス ライセンスの機能

PIX 525	R (制限付き)		UR (制限なし)				FO (フェールオーバー) ¹				FO-AA (フェールオーバー アクティブ/アクティブ) ¹			
ユーザ、同時	無制限		無制限				無制限				無制限			
セキュリティ コンテキスト	サポートなし		2 オプション ライ センス： 5 10 20 50				2 オプション ライ センス： 5 10 20 50				2 オプション ライ センス： 5 10 20 50			
IPSec セッ ション	2000		2000				2000				2000			
WebVPN セ ッション	サポートなし		サポートなし				サポートなし				サポートなし			
VPN ロード バランシング	サポートなし		サポートなし				サポートなし				サポートなし			
フェールオー バー	サポートなし		アクティブ/スタンバイ アクティブ/アクティブ				アクティブ/スタンバイ アクティブ/アクティブ				アクティブ/スタンバイ アクティブ/アクティブ			
GTP/GPRS	なし	オプション ライ センス： イネーブル	なし	オプション ライ センス： イネーブル			なし	オプション ライ センス： イネーブル			なし	オプション ライ センス： イネーブル		
最大 VLAN 数	25		100				100				100			
ファイアウォ ールの同時接続 ²	140 K		280 K				280 K				280 K			
最大物理イン ターフェイス数	6		10				10				10			
暗号化	なし	オプション ライ センス： 基本 (DES) 強化 (3DES/ AES)	なし	オプション ライ センス： 基本 (DES) 強化 (3DES/ AES)			なし	オプション ライ センス： 基本 (DES) 強化 (3DES/ AES)			なし	オプション ライ センス： 基本 (DES) 強化 (3DES/ AES)		
最小 RAM 容 量	128 MB		256 MB				256 MB				256 MB			

- このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアだけで使用できます。どちらの装置も同じモデルである必要があります。
- 同時ファイアウォール接続は、4つの接続すべてに対して1つのホストと1つのダイナミック変換を持つ80% TCPと20% UDPのトラフィック混合に基づいています。

表 A-8 PIX 535 セキュリティ アプライアンス ライセンスの機能

PIX 535	R (制限付き)		UR (制限なし)				FO (フェールオーバー) ¹				FO-AA (フェールオーバーアクティブ/アクティブ) ¹			
ユーザ、同時	無制限		無制限				無制限				無制限			
セキュリティ コンテキスト	サポートなし		2		オプション ライセンス:		2		オプション ライセンス:		2		オプション ライセンス:	
			5	10	20	50	5	10	20	50	5	10	20	50
IPSec セッション	2000		2000				2000				2000			
WebVPN セッション	サポートなし		サポートなし				サポートなし				サポートなし			
VPN ロード バランシング	サポートなし		サポートなし				サポートなし				サポートなし			
フェールオーバー	サポートなし		アクティブ/スタンバイ アクティブ/アクティブ				アクティブ/スタンバイ アクティブ/アクティブ				アクティブ/スタンバイ アクティブ/アクティブ			
GTP/GPRS	なし	オプション ライセンス: イネーブル	なし	オプション ライセンス: イネーブル			なし	オプション ライセンス: イネーブル			なし	オプション ライセンス: イネーブル		
最大 VLAN 数	50		150				150				150			
ファイアウォールの同時接続 ²	250 K		500 K				500 K				500 K			
最大物理インターフェイス数	8		14				14				14			
暗号化	なし	オプション ライセンス: 基本 (DES) 強化 (3DES/AES)	なし	オプション ライセンス: 基本 (DES) 強化 (3DES/AES)			なし	オプション ライセンス: 基本 (DES) 強化 (3DES/AES)			なし	オプション ライセンス: 基本 (DES) 強化 (3DES/AES)		
最小 RAM 容量	512 MB		1024 MB				1024 MB				1024 MB			

- このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアだけで使用できます。どちらの装置も同じモデルである必要があります。
- 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

セキュリティ サービス モジュール サポート

表 A-9 に、各プラットフォームでサポートされる SSM を示します。

表 A-9 SSM サポート

プラットフォーム	SSM モデル
ASA 5505	サポートなし
ASA 5510	10AIP SSM AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5520	10AIP SSM AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5540	10AIP SSM AIP SSM 20 CSC SSM 10 ¹ CSC SSM 20 ¹ 4GE SSM
ASA 5550	サポートなし (4GE SSM は組み込みであり、ユーザ取り外し不可能)
PIX 515/515E	サポートなし
PIX 525	サポートなし
PIX 535	サポートなし

1. CSC SSM ライセンスでは最大 1,000 ユーザをサポートでき、Cisco ASA 5540 シリーズ アプライアンスではさらに多くのユーザをサポートできます。CSC SSM を ASA 5540 適応型セキュリティ アプライアンスとともに展開する場合、スキャンする必要があるトラフィックにだけ CSC SSM が送信されるようにセキュリティ アプライアンスを設定してください。詳細については、「スキャンするトラフィックの指定」(P.22-9) を参照してください。

VPN 仕様

この項では、セキュリティ アプライアンスの VPN 仕様について説明します。この項では、次のトピックについて取り上げます。

- 「Cisco VPN Client サポート」(P.A-11)
- 「Cisco Secure Desktop のサポート」(P.A-11)
- 「Site-to-Site VPN 互換」(P.A-11)
- 「暗号標準」(P.A-12)

Cisco VPN Client サポート

セキュリティ アプライアンスは、多種多様なソフトウェアおよびハードウェア ベースの Cisco VPN Client をサポートします (表 A-10 を参照)。

表 A-10 Cisco VPN Client サポート

クライアント タイプ	クライアント バージョン
SSL VPN クライアント	Cisco SSL VPN クライアント、バージョン 1.1 以降
ソフトウェアの IPSec VPN クライアント	Windows 用 Cisco VPN Client、バージョン 3.6 以降 Linux 用 Cisco VPN Client、バージョン 3.6 以降 Solaris 用 Cisco VPN Client、バージョン 3.6 以降 Mac OS X 用 Cisco VPN Client、バージョン 3.6 以降
ハードウェアの IPSec VPN クライアント (Cisco Easy VPN リモート)	Cisco VPN 3002 ハードウェア クライアント、バージョン 3.0 以降 Cisco IOS ソフトウェア Easy VPN リモート、リリース 12.2(8)YJ Cisco PIX 500 シリーズ セキュリティ アプライアンス、バージョン 6.2 以降 Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス、バージョン 7.0 以降

Cisco Secure Desktop のサポート

セキュリティ アプライアンスは、CSD ソフトウェア バージョン 3.1.1.16 をサポートします。

Site-to-Site VPN 互換

多くのサードパーティの VPN 製品との相互運用性を提供することに加え、セキュリティ アプライアンスは、表 A-11 に示す site-to-site VPN 接続用の Cisco VPN 製品とも相互運用できます。

表 A-11 Site-to-Site VPN 互換

プラットフォーム	ソフトウェア バージョン
Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス	バージョン 7.0(1) 以降
Cisco IOS ルータ	リリース 12.1(6)T 以降
Cisco PIX 500 シリーズ セキュリティ アプライアンス	バージョン 5.1(1) 以降
Cisco VPN 3000 シリーズ コンセントレータ	バージョン 3.6(1) 以降

暗号標準

セキュリティ アプライアンスは、表 A-12 に示すものを含め、数々の暗号標準および関連するサードパーティの製品とサービスをサポートします。

表 A-12 暗号標準

タイプ	説明
非対称（公開キー）暗号化アルゴリズム	RSA 公開/秘密キー ペア、512 ～ 4096 ビット DSA 公開/秘密キー ペア、512 ～ 1024 ビット
対称暗号化アルゴリズム	AES : 128、192、および 256 ビット DES : 56 ビット 3DES : 168 ビット RC4 : 40、56、64、および 128 ビット
完全転送秘密（Diffie-Hellman キー ネゴシエーション）	グループ 1 : 768 ビット グループ 2 : 1024 ビット グループ 5 : 1536 ビット グループ 7 : 163 ビット（Elliptic Curve Diffie-Hellman）
ハッシュ アルゴリズム	MD5 : 128 ビット SHA-1 : 160 ビット
X.509 認証局	Cisco IOS ソフトウェア Baltimore UniCERT Entrust Authority iPlanet/Netscape CMS Microsoft Certificate Services RSA Keon VeriSign OnSite
X.509 証明書登録方法	SCEP PKCS #7 および #10